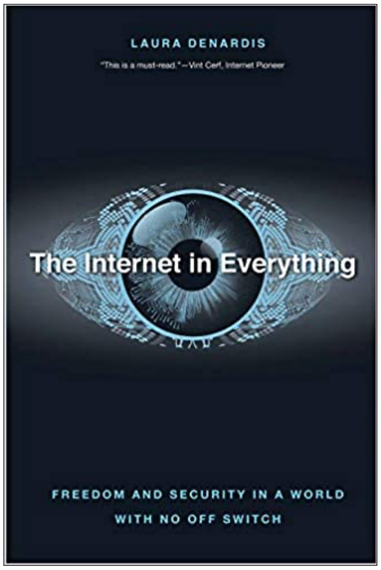
International Journal of Communication 15(2021), Book Review 1154–1156 1932–8036/2021BKR0009

Laura DeNardis, ***The Internet in Everything: Freedom and Security in a World With No Off Switch***, New Haven, CT: Yale University Press, 2020, 286 pp., $28.84 (hardcover), $17.60 (Kindle).

Reviewed by
Martha Isabel Falencik
University of Southern California, USA


LAURA DENARDIS
"This is a must-read."—Vint Cerf, Internet Pioneer
The Internet in Everything
FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH

In ***The Internet in Everything: Freedom and Security in a World With No Off Switch,*** Laura DeNardis enumerates the global threats, risks, ventures, pros, and cons of the Internet of things (IoT). This systematic evaluation of the relation between human communication and devices provides the reader with insight into the blurred boundaries between the tangible and cyber realms, security, and convenience.

The author asks: What does the IoT mean for consumer safety and national security? She unpacks the new complex threats associated with national security and privacy issues. This volume explores various "sides" of these issues, arguing that cybersecurity governance is needed while pleading to keep freedom of expression as wide-ranging as possible.

The Internet in Everything is organized as follows: "Part One: From Communication to Control" explains the post-Internet cyber-physical disruption. It compares the foundational policy of "universal" Internet against the fragmentation in the IoT (p. 11). It argues that fragmentation in the IoT can serve as a check on security weak spots in global networks. "Part Two: The Global Politics of Cyber-Physical Systems" explains new aspects of privacy, cyber-physical security, and interoperability politics. It exposes the dangers of ransomware and the need to balance law enforcement access to data. It exposes the ecosystem in which IoT consumers become dependent on one vendor to meet their cyber-physical needs. Part three redefines Internet freedom and explains the direction in which global Internet governance should proceed at the "cyber-physical policy moment" (p. 198). It sheds light on the Internet shift from a communication network to a control network embedded in the physical world and its use as a tool for political power. This section suggests that policy attention needs to shift from digital content to digital infrastructure.

In *The Internet in Everything*, the importance for economic growth, individual rights, business models, and governance are posited as an "opportunity to shape the constitution of this future." (p. 8). Still, it is important to recognize that "cyber interconnections in material objects makes systems traverse national boundaries in a way that can complicate jurisdiction" (p. 13). Many questions remain, but DeNardis does clarify why governance is a viable way to construct some resemblance of stability in the IoT.

The author infuses novel-like fear by sequentially mentioning the systems in which cyber-physical disruption is heterogeneous, clearly convenient, and thus impossible to resist. She contends that the IoT will intrude on human life, whether people want it to or not. This is debatable. Perhaps it is possible to prevent IoT from invading one's life. At least, consumers need to consider cybersecurity before bringing smart, interactive, interconnected toys into their personal spaces or risk child exploitation, identity fraud, and government surveillance from around the world. Yet, often, these devices are optional and so trivial that the consumer may reject them.

The author also praises the utility of cyber-physical systems as they relate to innovation and performance, which feeds off the IoT's collection of massive amounts of data. The same innovations that undermine the privacy of home help the disabled and elderly, and strengthen the agriculture sector by reducing the need for pesticides, maximizing food output, and reducing water consumption. These new technologies can flag a leak that would otherwise result in environmental disaster. Cyber-physical systems also enhance police efficacy when license-plate readers identify stolen vehicles or wanted felons.

The author acknowledges the complicated conundrum these pros and cons of cyber-physical systems present. IoT makes consent complex and often unattainable. She insists that

> the challenges in the cyber-physical domain connect variously to a patchwork of concerns: discrimination, government surveillance, foreign intelligence, boundary control, anonymity, confidentiality, personal information dissemination, safety and health, harassment, identify formation, and the right to be left alone. . . . Public policy views the advantages of massive data collection as a public good while viewing the harms in the same context as an individual problem. Cyber-physical systems present the greatest privacy complications ever to confront humanity. (p. 88)

The *Internet in Everything* unpacks the cumulative potential energy of state cyber-offense capability as a growing problem over time. Politically engineered code, knowledge of vulnerabilities, and exploit stockpiling build on unspoken codes of conduct that have allowed software and hardware manufacturers some leeway for correction. Today the hoarding and stockpiling of digital vulnerabilities is the norm, which creates "even greater concerns for human security and internet stability" (p. 98). The remaining unanswered questions leave a void of uncertainty about human security, human safety, and the role the cyber-physical infrastructure plays in the global digital economy and its democracy.

Communication networks are rapidly evolving into control networks that are seeping into homes and private spaces. For DeNardis, this change translates into political power: "The blurring of boundaries between the physical and virtual realms is also blurring understandings and affordances of the internet itself" (p. 188). The Internet is a collection of independent networks owned and operated by private companies, which raises questions about the power struggles between governments and private industries such as AT&T, Comcast, Vodafone, Facebook, and Google. This is clear in the way technology deciphers the linguistic code-shifting of "cyber" versus "Internet." While "cyber" is used in international conflict interactions or in a national security context, the term "Internet" is used to discuss technical architecture, social media propaganda, censorship, access, or intellectual property.

DeNardis lays out the interconnection between cyber intersectionality and public policy. She contends that central authority could successfully regulate cryptocurrencies and other decentralized systems. But she worries that without transparency, greed and the thirst for power will subvert the IoT. Thus, DeNardis's *The Internet in Everything* continually stresses the importance of shifting from digital content to digital infrastructure.

The book would appeal to academics and a wider public. It provides a clear view of consumer safety, privacy issues, national security, and the development of Internet governance. It also unpacks the controversy between the irresistible conveniences of IoT and the dangers that come with the inevitable surrender to it. It is a thorough, accessible read.